

# United States District Court

for the  
Western District of New York

**United States of America**

**v.**

**Case No. 20-mj- 183-HKS**

**MICHAEL REGAN**

---

*Defendant*

## **CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

### **COUNT 1**

#### **(Production of Child Pornography)**

On or about the date of August 27, 2020, in the County of Erie, in the Western District of New York, the defendant, MICHAEL REGAN, did employ, use, persuade, induce, entice, or coerce a minor to engage in, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, knowing or having reason to know that such visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, in violation of Title 18, United States Code, Sections 2251(a).

### **COUNT 2**

#### **(Enticement of a Minor)**

On or about the date of August 28, 2020, in the County of Erie, in the Western District of New York, the defendant, MICHAEL REGAN, using facilities and means of interstate and foreign commerce, that is, a cellular telephone and the internet, did knowingly persuade, induce, entice, and coerce, and attempt to persuade, induce,

entice, and coerce a minor female victim known to the government, an individual who has not attained the age of 18 years, to engage in sexual activity for which any person can be charged with a criminal offense, in violation of Title 18, United States Code, Sections 2422(b).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

  
Complainant's signature

RANDALL E. GARVER  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION

*Printed name and title*

Sworn to before me and signed telephonically.

Date: December 3, 2020



*Judge's signature*

City and State: Buffalo, New York

HONORABLE H. KENNETH SCHROEDER, JR.  
UNITED STATES MAGISTRATE JUDGE

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF A  
CRIMINAL COMPLAINT AND SEARCH WARRANTS**

STATE OF NEW YORK    )  
COUNTY OF ERIE        )    SS:  
CITY OF BUFFALO        )

**I. INTRODUCTION**

I, RANDALL E. GARVER, after being duly sworn, depose and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation and entered on duty in May 2006. I am currently assigned to the Buffalo Field Office and work on cases associated with the Violent Crimes Against Children program, which targets individuals involved in the online sexual exploitation of children. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, 2423, and 2261. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child sexual abuse material (CSAM), Sexual Enticement, Travel to Engage in Illicit Sexual Conduct, and Cyberstalking laws in which computers or smartphones/devices are used for engaging in such violations of Federal law.

2. This affidavit is made in support of a criminal complaint charging **MICHAEL REGAN**, date of birth **XX/XX/1982**, with violations of Title 18, United States Code, Sections 2251(a) [Production of Child Sexual Abuse Material] and 2422(b) [Enticement of a Minor].

3. This affidavit is further made in support of search and seizure warrants, pursuant to Rule 41 of the Federal Rules of Criminal Procedure to search the following premises, where I believe evidence of violations of Title 18, United States Code, Sections 2251(a) [Production of Child Sexual Abuse Material] and 2422(b) [Enticement of a Minor] will be located:

- a. **The person of MICHAEL REGAN, date of birth XX/XX/1982;**
- b. **A gray 2020 Jeep pickup truck bearing New York registration KDK 3697, registered to Alquita Janei Regan, address 5112 Sheridan Drive, Williamsville, New York 14221; Vehicle Identification Number (VIN) 1C6HJTAG7LL184909;** the FBI also seeks to seize this vehicle, as it was used in furtherance of a crime.
- c. **5112 Sheridan Drive, Williamsville, New York 14221,** the residence of **REGAN**

4. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint and search warrants, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251(a) [Production of Child Sexual Abuse Material] and 2422(b) [Enticement of a Minor] exists at the target premises and that **REGAN** violated the same statutes.

## **II. COMPUTER TERMS USED IN THIS AFFIDAVIT**

5. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (ISP) that connects to the Internet. The ISP assigns each user an Internet Protocol (IP) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Thus, by ascertaining the IP address relating to a specific message sent or action taken over the Internet, it is possible to determine the ISP and even the individual computer responsible.

6. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and

history files of the browser used. Additionally, a computer also creates logs, indices, and registries indicating when a computer was used, which user was logged on, and when data was accessed, shared, transferred, or downloaded. A forensic examiner can often recover internet search history, chat sessions, and e-mails sent from the computer. Cellular telephones also allow the user to save or store text messages and e-mail messages received by the phone, for later viewing or distributing, and even if deleted, a forensic examiner can often recover evidence of such text messages and e-mail messages.

7. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

8. “Social networking” or “social network service” is a term used to describe applications or websites which focus on establishing networks or relationships among individual users based on interests or activities. These services typically consist of a personal online representation of an individual, often referred to as a profile, a list of other individuals with which a person has interests or allowed to view their profile, and a variety of other capabilities, such as the upload and sharing of images and videos. Newer capabilities allow access to the social networks via mobile devices such as cellular telephones and the upload of real-time information to an individual's profile. Most, if not all, of the social networks are accessible via the Internet and allow a member to contact other members via e-mail, instant messaging, or comments placed directly to a member's profile. Normally, information posted by individuals to their own or another individual's profiles are not vetted for accuracy or content. Discussed herein is an application (“app”) called TextNow which is downloaded to a phone or mobile device such as an Apple iPod. Individuals then use the device’s WiFi connection to enable texting and voice calls. From the app, users can even send pictures and videos, along with their chat/text conversation.

## **II. PROBABLE CAUSE**

9. The investigation to date has shown that there is probable cause to believe that **REGAN** used his TextNow account, 17165995051, to knowingly engage in a sexual conversation with a 13 year-old-girl (hereinafter, “Victim”) wherein **REGAN** requested and received nude images that constituted child sexual abuse material (CSAM, formerly child pornography) from Victim and enticed the same Victim into sexual contact.

10. On December 2, 2020, the FBI's Child Exploitation Task Force initiated this investigation after Buffalo Police Department (BPD) requested assistance. The same day, my colleague and I met with an Erie County Assistant District Attorney (ADA) in her office. The ADA provided us with the results of BPD's consent search of Victim's iPod, along with investigative reports and notes. My colleague and I immediately reviewed the findings and located a TextNow conversation between Victim and **REGAN**. The below paragraphs were developed based upon my review of this conversation.

Chat Conversation:

11. On August 5, 2020, the conversation began after the pair met over Snapchat weeks before. Victim wrote, "hey Jason it's me [Victim true first name]"; **REGAN** replied "I can't believe you touched your self sucking his dick and cam lol...Lol u want to do it again I bet." **REGAN** asked Victim about getting a nude picture of Victim's mother or a classmate from school and Victim asked why he wanted to see "tits", to which **REGAN** replied, "I love them. And I've never seen young tits before." **REGAN** then asked about getting a picture of Victim's mother's or a friend's breasts, or a picture of a friend sucking on something. Victim stated that she only wanted **REGAN** to see her and he replied, "I only wanted you to suck my cock and your showed yourself to your stepdad without him asking. And sucked his dick." **REGAN** then asked if Victim knew a girl that lived off William Street near a particular pizza restaurant, which she recognized as her friend. **REGAN** wrote, "that was the girl my buddy fucked. I think if that's her."

12. On or about August 18, 2020, the conversation continued with **REGAN** writing, "so mad at you...tried to set me up." Victim wrote back, "U wanted something I



didn't want to do...I would've done it." **REGAN** asked "what" and Victim replied, "I would've sucked ur dick...but u asked for something I just didn't want to do." She then agreed that she would still perform oral sex on **REGAN**. After receiving a picture of Victim holding her sweatshirt up exposing her bra, **REGAN** wrote "Damn. Take that off...want to know you still want me. Show me those tits." Victim replied by sending a picture of her breasts. He next asked, "when can you suck my cock", before writing, "show me [that] tight pussy" which Victim refused until she saw a picture of **REGAN**'s face. After a reference to previously sending pictures and videos, **REGAN** replied they were all on Snapchat and deleted. Victim then mentioned that she was recently in trouble with law enforcement and **REGAN** wrote "I mean I'm a cop we wouldn't do that in Cheektowaga." As the conversation continued, Victim wrote that she had sexual contact with a young adult at a party. **REGAN** asked, "did he cum...what was he saying when you were sucking it." **REGAN** accused Victim of lying about sexual contact and wrote, "show me your pussy I want to believe you". Victim resisted, stating she would do so in "real life" and sent a picture of her exposed breast.

13. On or about August 19, 2020, the conversation continued with **REGAN** writing, "can't stop jerking off to your pics. So what's really your deal. Why do you want to suck my dick so bad. How many dicks have you really sucked. And who's. Please be honest. I really like you." After Victim answered him, **REGAN** wrote "how are you gonna suck it...can I finger you...still want me to fuck you". **REGAN** then mentioned the friend that the two discussed above and told Victim that he had vaginal and oral sex with the girl. He then wrote to Victim "what school do you go to what grade are you in"; Victim replied, "8<sup>th</sup> grade

and a private school.” **REGAN** next asked, “wait so your going into 8<sup>th</sup> grade?...and you and [REDACTED] are in the same grade?”, referring to Victim’s friend discussed above. Victim advised that she is in the same grade as her friend that **REGAN** claimed to previously have oral and vaginal sex with – he stated that the girl advised she was going into high school when the sex occurred last summer (2019). **REGAN** then asked, “so your 14...so she was 13 last year then?” Victim and **REGAN** then continued to discuss age with Victim advising she was 13 years old; he asked “yea so your 13 now” and Victim confirmed, “yeah”. **REGAN** replied, “oh well she sucked my dick good and her pussy tasted and felt so good.” Victim replied, “mine will taste better...when can u fuck me”. **REGAN** asked for Victim’s address and she provided it and advised she could only be out until 5:30 pm but could sneak out to meet **REGAN**. **REGAN** next wrote, “Dam. [Victim true first name] I want you so fucking bad but I’m nervous”. **REGAN** asked for a video from Victim and wrote that he wanted her to “suck my cock and swallow my cum while I touch your pussy”. **REGAN** wrote that they could not meet that evening because he had to work but again asked for a video, “take your clothes off in it and say you want this daddy.” After some delay, **REGAN** asked “when are you gonna make it I want to jerk off to [you].” From the chat log, it appears as though Victim sent a video, but the contents were not recovered by the FBI. **REGAN** replied, “Omg [Victim true first name] I love you”. **REGAN** commented that Victim’s younger brother was audible in the video and then asked if she could perform oral sex on the brother, “to bad he wouldn’t let you suck his dick I wanted to see [that].” **REGAN** then asked if Victim’s brother would want to perform oral sex on him as well and again asked about her doing the same: “I want to see u suck him for 10 seconds”. Victim wrote that she wanted **REGAN** all to herself and he wrote, “I want to cum in that little pussy...show me.” Victim then sent a video, the

contents of which were not recovered. Victim replied, “U can fuck it” to which he replied “I want to. And cum in it.”

14. On or about August 20, 2020, **REGAN** wrote, “God that video is hot...I want you to suck that dildo...want to see all that slobber and gag...I want to cum in your mouth pussy and ass.” **REGAN** next asked Victim if she would be willing to have anal sex with him and wrote, “let me see your ass. Be naked and bend over in front of your phone in a video and spread your cheeks.” **REGAN** wrote that he was going to love having intercourse with Victim and she asked when that may be. **REGAN** wrote that he was hoping for today (August 20) and Victim advised she was free between 2 pm and 5 pm. Victim wrote that she was not on birth control so **REGAN** could not ejaculate in her vagina; he wrote that he would only do so in her rectum. **REGAN** next wrote, “show me baby. Show me you want my cock. That dildo is the size of my cock...take it all the way and spit all over it...as far as u can baby. I want to see you gagging. Like the video all wet and sloppy...that’s what daddy wants.” Victim wrote back, “yes sir” along with a video (contents not recovered).

15. On or about August 25, 2020, **REGAN** asked, “baby can you suck my cock Friday” and Victim advised she was free that morning. **REGAN** replied, “we will fuck. I want. To cum in your mouth first.” Victim then sent two pictures of her breasts at **REGAN**’s direction.

16. On or about August 26, 2020, **REGAN** asked Victim “could you walk down to the end of your street at the corner of William?” Victim asked, “On Friday?” and he replied,

“yes.” Victim asked if she could call **REGAN** and he replied he could not because a friend was over. When Victim suggested he tell the friend that Victim is his niece, **REGAN** wrote “don’t want him knowing I’m gonna get my dick sucked by a 13 year old.” **REGAN** wrote, “and your gonna have to meet me at William. I don’t want to be in your street. Just in case anyone see you get in my car or in case of anything.” He told Victim she could not use her phone in his car and could not take any pictures. **REGAN** wrote, “I think your sexy as fuck I’m gonna want you [a lot]. Sucks so young but I can’t get in trouble. Has to be our secret baby.” When referring to his having sex with Victim’s minor friend last summer, **REGAN** wrote, “Not gonna lie get [sucked] off and eating her pussy and fucking her was fun. That was the first time I ever did anything with someone that young. But you are so much sexier and your body puts [hers] to shame. It’s gonna be a 100 times better with you.” Next **REGAN** wrote to Victim that years ago he put his thumb inside his niece’s vagina while the two were horse playing in the pool. He wrote to Victim that he then went into the house with his niece to apologize and the girl said she enjoyed it; **REGAN** then wrote that he had sex with the girl, “so yes I fucked 2 13 year old one 8 years ago and one last summer. You don’t think I’m a creep do you”. He continued, “I feel like a creep. I was 17 years older and 20 years older than them” before telling Victim he is now 37 years old and was 30 and 36 years old when the recounted incidents occurred; **REGAN** said he will be “24 years older than you when you suck me off.” **REGAN** then discussed wanting Victim to record a sexual act with her stepdad to share with him.

17. On or about August 27, 2020, **REGAN** wrote, “U still want to suck my cock tomorrow” and Victim said “yes...I’ll never turn that down”. **REGAN** asked that Victim

wear “loose shorts no panties or bra...so I can touch your pussy”. He then wrote “send me a tits and face pic and pussy. So I know your serious about tomorrow.” Victim sent a picture, which I reviewed, of a close-up image of her vagina with her fingers spreading the labia open. **REGAN** wrote, “send me a video too please. Want to hear you say I want to suck your cock daddy”; Victim sent a video, which the FBI did not recover. **REGAN** wrote, “honest answer. Why do you want to suck my cock so bad being 24 year older than you.”

18. On or about August 28, 2020, **REGAN** wrote, “Get naked. Send me a video. Full body naked and say daddy I’m ready to suck your cock. You want to suck on my 13 year old tits [and] play with my virgin pussy.” Victim replied, “I need to shower so come at 10:25”. Victim replied, “Omg. Baby. Show me that ass. Bend over and spread it.” Victim then sent an image, which I reviewed, of her nude, bent over facing away from the camera spreading her buttocks exposing her vagina. **REGAN** next wrote, “so nervous” and Victim replied, “I’m walking now.” **REGAN** replied, “Ok. I’m nervous”; Victim wrote, “don’t be...I’m almost there.” 14 minutes later, Victim wrote “that was nice” and **REGAN** wrote “was amazing.” Victim replied, “Ur cum was delicious.” **REGAN** wrote that he was so nervous he could not get a full erection and Victim asked, “how’d my pussy taste?” **REGAN** wrote “make sure you delete my texts and stuff too...no need for evidence lol”.

19. On or about August 31, 2020, **REGAN** wrote to Victim that he had sexual contact with his two nieces, ages 16 and 12. **REGAN** then recounted various purported sexual scenarios with his nieces and again asked for videos of Victim, which she sent (contents not recovered). The following day, September 1, 2020, the two discussed whether Victim

would be willing to have sexual contact with **REGAN** and his nieces. Victim sent a nude image of her vagina and breasts to **REGAN** after he told her to masturbate in the bathroom. Victim sent several videos and two nude images during the sexual conversation, though she was not specifically directed to do so. **REGAN** wrote, “babe I have had more sex in the last few days than few years because of you,” though it does not appear, from the chats, that the two met again (in the conversations regarding his nieces, **REGAN** discussed various sexual encounters). In fact, soon thereafter, Victim again asked **REGAN** to get together for intercourse.

20. On or about September 3, 2020, **REGAN** suggested meeting Victim for sex with one of his minor nieces. He stated that the niece wanted to bring her 11-year-old friend, “her friends only 11. I can’t risk that lol.” **REGAN** wrote Victim, “[Purported niece] wants you to send a video of you opening up your pussy and saying u want to lick this pussy before your uncle fucks me.” Victim replied, “she wants me to send a video saying that then she’ll pick me up????” Victim sent a video, the contents of which were not recovered, and **REGAN** replied, “God damn”. Based on my experience and review of the chat log, I believe it is possible that this portion of the chat was an attempt by **REGAN** to get more sexual conversations, pictures, and videos from Victim, and not a true attempt to have her engage in any sexual contact with his purported nieces.

#### Additional Analysis:

21. On December 2, 2020, the FBI issued an emergency disclosure to TextNow requesting account details of 17165995051. The same day, TextNow disclosed to the FBI

that the account is registered to username “mrsnipes89”, email address mrsnipes89@yahoo.com, and provided that the account was created on June 20, 2020 from IP address 108.17.5.55, which is administered by Verizon Landline. The same day, the FBI issued an emergency disclosure to Verizon Landline for this IP address; Verizon provided that on June 20, 2020, the IP address was registered to **MICHAEL REGAN, 5112 Sheridan Drive, Williamsville, New York 14221.**

22. From the same TextNow return, the FBI learned 272 IP logs were entered between November 21, 2020 and December 2, 2020. As none of these dates corresponded to the subject conversations (in August 2020), the FBI selected three IP addresses logged by TextNow on December 2, 2020: 108.17.59.41, 72.45.250.51, and 174.224.140.77, administered by Verizon Landline, Charter Communications, and Verizon Wireless, respectively.

23. Emergency disclosures were issued to each of these providers with the following results. On December 2, 2020, an official with Charter Communications called me and told me that IP address 72.45.250.51 was registered to Wegman’s, address 5275 Sheridan Drive, Williamsville, New York at the time of the TextNow IP log. The same day, Verizon Landline disclosed to the FBI that IP address 108.17.59.41 was registered to **MICHAEL REGAN, 5112 Sheridan Drive, Williamsville, New York 14221**, and provided phone number (716) 398-2181, and email address beast8913@icloud.com with the return. Finally, on December 2, 2020, officials with Verizon Wireless advised that IP address 174.224.140.77 was a natting IP, meaning multiple cellular telephones were accessing their network from the

IP address. Pursuant to the emergency disclosure, Verizon Wireless provided 132 telephone numbers that were accessing the network from IP address 174.224.140.77 at the specifically requested time. Included in the 132 numbers was telephone number (716) 398-2181, which is **REGAN**'s number, as it was provided with Verizon Landline's return (stated above). A subpoena was issued to obtain subscriber information for telephone number (716) 398-2181; the results have not been received.

24. On September 29, 2020, Victim was subjected to a forensic interview at the Child Advocacy Center (CAC) in Buffalo. The interviewer asked Victim if she knew who "Jason" was, and Victim replied that he is a sexual predator who she knows as the father of her friend, "Taylor." Victim said "Jason" asked for pictures of her, but Victim did not send them. Victim said "Jason" was a Cheektowaga Police Department officer and had sleeve tattoos on both arms with an eagle in one. Prior to the interview, Victim's mother told the BPD detective that she learned from Victim that "Jason" drove a black, Jeep truck with oversized tires and LED wheel wells.

25. On December 2, 2020, an FBI Agent drove by **5112 Sheridan Drive, Williamsville, New York 14221** and observed a **gray 2020 Jeep pickup truck bearing New York registration KDK 3697, registered to Alquita Janei Regan, address 5112 Sheridan Drive, Williamsville, New York 14221; Vehicle Identification Number (VIN) 1C6HJTAG7LL184909**. On December 3, 2020, the same Agent drove by the house and observed the same vehicle and took a picture. The Jeep pick up was observed to be dark gray and had oversized tires that stuck out distinctively from the vehicle body.



26. On December 3, 2020, my colleague and I interviewed Victim at her residence in Buffalo. During the interview, Victim described “Jason” as being a tall, white, male, with “blondish brown” hair who was “scruffy” but did not have a beard. Based on our investigation we know “Jason” to be a pseudonym for **REGAN**. She recalled **REGAN** had “sleeve” tattoos on both arms and an eagle in one; he sent her one picture of his tattoos on Snapchat, but Victim no longer had the image. Victim confirmed she had sexual contact with **REGAN** in August 2020. On that particular day, he drove to Ludington Street in Buffalo and parked across from Willie’s, a tavern located at the corner of Ludington Street and Gold Street. Victim observed a dark gray Jeep truck with “fat tires” that extended beyond the vehicle frame. She recalled that the wheel well could be lit up with LED lights. I showed her a picture that was taken earlier in the morning by an FBI Agent at **5112 Sheridan Drive, Williamsville, New York 14221**, and Victim readily agreed that was the truck she had sexual contact with **REGAN** in (the image was of the **gray 2020 Jeep pickup truck bearing New York registration KDK 3697, registered to Alquita Janei Regan, address 5112 Sheridan Drive, Williamsville, New York 14221; Vehicle Identification Number (VIN) 1C6HJTAG7LL184909**). Victim recalled she previously knew “Jason” as the father of her friend “Taylor” who was two years ahead of her at her previous school, and likely now in 10<sup>th</sup> grade. Victim attends a different school and has not spoke to “Taylor” in years. Victim said sometime in July, “Jason” added her on Snapchat and the two corresponded for a few weeks before he suggested they move the conversation to TextNow. On Snapchat, “Jason” did not initially identify himself as Taylor’s father. After the sexual encounter with **REGAN**, he told Victim “if someone finds out I’m talking to you, I’ll come to your house.” Victim did not know the nature of the threat but said she knew to “keep it to myself.”

27. Searches conducted by FBI intelligence analysts found that **REGAN** is listed in Accurint as a resident of **5112 Sheridan Drive, Williamsville, New York 14221**. A check of National Fuel, a local gas provider, showed that service to **5112 Sheridan Drive, Williamsville, New York 14221** is active, and the account is in the name of Alquita Regan, **REGAN's** wife.

28. This warrant seeks authorization to search **5112 Sheridan Drive, Williamsville, New York 14221** to seize electronics and digital media related to these target offenses. However, I know TextNow is primarily used on cellular (mobile) phones. Evidence related to **REGAN's** conversations with Victim, his possible nieces, the friend he claimed to have had sexual contact with, would likely be located on the phone, which could possibly be located on **REGAN's** person. It is, therefore, essential to the investigation, to search **the person of MICHAEL REGAN, date of birth XX/XX/1982** to seize his cellular telephone that contains the TextNow application or any other digital media on his person. Additionally, as the sexual contact occurred inside **REGAN's** Jeep truck, it is also essential to the investigation to seize and search the **gray 2020 Jeep pickup truck bearing New York registration KDK 3697, registered to Alquita Janei Regan, address 5112 Sheridan Drive, Williamsville, New York 14221; Vehicle Identification Number (VIN) 1C6HJTAG7LL184909.**

Biometric Authorization

29. The warrant I am applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

- a) I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b) If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c) If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d) If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based

on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e) In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f) As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g) I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- h) In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible

that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

- i) Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

### **III. CONCLUSION**

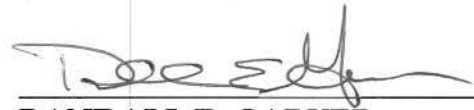
30. Based upon the above information, I assert that probable cause exists to believe that **MICHAEL REGAN** knowingly violated Title 18, United States Code, Sections 2251(a) [Production of Child Sexual Abuse Material] and 2422(b) [Enticement of a Minor].

31. Additionally, I assert that probable cause exists that violations of Title 18, United States Code, Sections 2251(a) [Production of Child Sexual Abuse Material] and 2422(b) [Enticement of a Minor] now exist at/on:

- a. **The person of MICHAEL REGAN, date of birth XX/XX/1982;**

- b. A gray 2020 Jeep pickup truck bearing New York registration KDK 3697, registered to Alquita Janei Regan, address 5112 Sheridan Drive, Williamsville, New York 14221; Vehicle Identification Number (VIN) 1C6HJTAG7LL184909; which the FBI also seeks to seize, as it was used in furtherance of a crime.
- c. 5112 Sheridan Drive, Williamsville, New York 14221, the residence of REGAN

32. In consideration of the foregoing, I respectfully request that this Court approve the Criminal Complaint and Arrest Warrant for MICHAEL REGAN and that said Complaint and Arrest Warrant be sealed until further order of this Court and that all papers submitted in support of this Application, including the Application, Affidavit, and Arrest Warrant remain under seal until further order of this Court. Additionally, I respectfully request that this Court approve the warrants seeking the search of the above listed property/premises and the seize of the target vehicle listed in letter b, above.

  
\_\_\_\_\_  
RANDALL E. GARVER  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed telephonically

this 3<sup>rd</sup> day of December 2020.

  
\_\_\_\_\_  
HON. H. KENNETH SCHROEDER, JR.  
United States Magistrate Judge